AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph starting on page 11, line 5 with the following:

Several components may be employed in an extranet system to provide certain extranet capabilities and functions. For example, a firewall server may provide firewall protection for the extranet. Commercially available systems, such as ~~Checkpoint Firewall-1~~ CHECKPOINT FIREWALL-1 or another firewall component may be employed in this capacity. In certain embodiments, one firewall may divide the extranet from external networks, such as the Internet, and a second firewall may divide the extranet from corporate networks, such as intranets and fileservers. Another component may be a web server, a functionality which may be provided by ~~Netscape Enterprise Server~~ NETSCAPE ENTERPRISE SERVER or an equivalent component. A separate extranet web server may also be utilized. ~~Netscape Enterprise Server~~ NETSCAPE ENTERPRISE SERVER, MS IIS, or any other extranet web server system may fulfill this function. A certificate authority (CA) server, such as ~~Cybertrust Enterprise~~ CYBERTRUST ENTERPRISE CA, may be included to provide authentication services or to issue digital certificates. An LDAP (Lightweight Directory Access Protocol) or other suitable directory can be implemented using a directory server such as ~~Netscape Directory~~ NETSCAPE DIRECTORY, ~~Isocor~~ ISOCOR, or other LDAP servers. An extranet database may be maintained using a component such as ~~Oracle8i~~ ORACLE8I or another suitable database server. A number of components are available to provide access control functionality, such as ~~Netegrity SiteMinder~~ NETEGRITY SITEMINDER, ~~enCommerce getAccess~~ ENCOMMERCE GETACCESS, ~~Entegrity~~ ENTEGRITY, ~~Aventail~~ AVENTAIL, MS IIS, and ~~Netscape Enterprise Server~~ NETSCAPE ENTERPRISE SERVER. Other access control policy servers will be known to those of skill in the art and may be used in this capacity.

Please replace the paragraph starting on page 14, line 5 with the following:

In certain embodiments, a certificate, such as a certificate authenticating the identity of the user or the extranet, is stored on a separate device, such as a smart card. Suitable technologies include the ~~iKey~~ IKEY from ~~Rainbow Technologies~~ RAINBOW TECHNOLOGIES, and the ~~Aladdin Smartcard Environment~~ ALADDIN SMARTCARD ENVIRONMENT, among others. In certain embodiments, the certificate is a certificate issued by a certificate authority associated

with the extranet. In certain embodiments, information stored on the device cannot be directly accessed by the user. A certificate-bearing device may further include information such as a URL or other address for the extranet, attributes or preferences of the user, a source or issuer, e.g., the root, of the certificate, or other suitable information. Certificate-bearing devices may be further protected by requiring a password for use. Thus, in one exemplary embodiment, a certificate-bearing device, when coupled to a user's computer system, prompts the user to provide a password. Additionally, upon entry of the correct password, the device may launch an application, such as a web browser, and connect the user to the extranet. In instances where a public key/private key pair is used, the private key may be stored on the certificate-bearing device in a way that is inaccessible to the user so that the user is inhibited from duplicating or distributing copies of the private key.

Please replace the paragraph starting on page 15, line 14 with the following:

An extranet as described above, optionally including a security application, may be assembled in any of a variety of configurations. For example, Figure 2 depicts one example of an extranet bundle configuration 200. A user 210 connects via the Internet 120 and a channel service unit/data service unit (CSU/DSU) 212 to an extranet 200. The connection is handled by a router 230 and proceeds through a firewall server 232. The firewall server 232 may be connected by hubs 234 to an extranet web server 240 and a directory server 242, a certificate authority (CA) web server 250, an access control policy server 260, and a certificate authentication server 262. Other configurations for an extranet bundle will be apparent to those of skill in the art and are intended to be encompassed by the present invention. In an exemplary embodiment, the firewall server 232 may be ~~CheckPoint Firewall-1~~ CHECKPOINT FIREWALL-1 4.0, the extranet webserver 240 may include ~~Netscape Enterprise Server~~ NETSCAPE ENTERPRISE SERVER 3.61, ~~Netegrity SiteMinder~~ NETEGRITY SITEMINDER 3.5.1 Web Agent, or ~~ValiCert Web Server Validator~~ VALICERT WEB SERVER VALIDATOR 2.5, the directory server 242 may be ~~Netscape Directory Server~~ NETSCAPE DIRECTORY SERVER 4.0, optionally with ~~ValiCert~~ VALICERT OCPS VA 2.0 for certificate validation, and the certificate authentication server 262 may be ~~Enterprise~~ ENTERPRISE CA 3.4.1, although other suitable components will be known to those of skill in the art and may be substituted for any of the foregoing components. The

bundle may additionally be configured to run a security application such as ~~CyberTrust Vault~~ CYBERTRUST VAULT with ~~Oracle Workgroup Server~~ ORACLE WORKGROUP SERVER 8.0.5, or any other applications, as desired. The function of the CA webserver 250 may be performed by ~~Netscape Enterprise Server~~ NETSCAPE ENTERPRISE SERVER or by a separate component, as is known in the art.

Please replace the paragraph starting on page 17, line 6 with the following:

In the configurations described above, a firewall is used to provide a secure barrier between the Internet and the extranet. As shown in Figure 4A, an additional firewall as described above may be used to separate the extranet from a corporate network, such as an intranet. In the configuration shown in Figure 4A, a certificate authority server 462 may be connected through a directory 490 to an access control policy server 460. The policy server 460 may be linked to a web server 440 linked to an extranet database server 444. The web server 440 may be linked to the corporate network 404 through the firewall 408. In this configuration, access to applications or data located on an intranet or database may be obtained using real-time access or data replication. ~~Netegrity SiteMinder~~ NETEGRITY SITEMINDER and ~~enCommerce getAccess~~ ENCOMMERCE GETACCESS are examples of components which may be used for this type of access. The function of a CA server may be performed, as described above, by an external CA hosting service, as depicted in Figure 4B.

Please replace the paragraph starting on page 17, line 20 with the following:

Alternatively, access may be proxy server-based, by using a proxy server as depicted in Figure 4C. A client 406 may connect through an extranet firewall 434 to a proxy server 496 and a CA server 462. The CA server 462 may be connected to a directory 490, which is also linked to the proxy server 496 through a proxy-based access control 498. Access may then be obtained via the World Wide Web, FTP, or other protocols. ~~BankOne~~ BANKONE, GTE ~~Aegis~~ AEGIS, NCP, and ~~Aventail~~ AVENTAIL are examples of components which may be used in conjunction with proxy server access. The proxy server 496 may also connect through the corporate firewall 408 to a backend application 416, located within the company's network.

Please replace the paragraph starting on page 20, line 2 with the following:

Next, extranet components may be selected to meet the particular needs of the organization 510. These components may include any of the components described above. In particular, the selection of an access control package may be based on any number of factors. Different access control packages offer different advantages and possibilities. ~~Netegrity SiteMinder~~ NETEGRITY SITEMINDER V3.6 offers multiple web servers with multiple applications and LDAP compatibility. ~~SiteMinder~~ SITEMINDER V3.6 is particularly suitable for organizations which prefer C++, or use ~~Bluestone~~ BLUESTONE or ~~Allaire~~ ALLAIRE. ~~enCommerce getAccess~~ ENCOMMERCE GETACCESS V3.0 also supports multiple web servers with multiple applications, supports CORBA (Common Object Request Broker Architecture), and is well suited to organizations which prefer Java, or use HAHT or ~~NetDynamics~~ NETDYNAMICS. ~~Entegrity AssureWeb~~ ENTEGRITY ASSUREWEB may be employed when other ~~Entegrity~~ ENTEGRITY products are in use, signed messages are required, strong international encryption is desired, or the organization prefers to avoid cookies. ~~Netscape Enterprise Server~~ NETSCAPE ENTERPRISE SERVER V3.x or ~~Microsoft~~ MICROSOFT IIS 4.0 may be preferred choice when central user management is not required, or access control is required for a single web server. ~~Aventail ExtraNetCenter~~ AVENTAIL EXTRANETCENTER offers access to back-end applications that may be unavailable using other software packages.